Alert

Prepared by the
Internet Crime Complaint Center (IC3)

November 17, 2005

NEW LEVEL OF SOPHISTICATION IN PHISHING SCAMS – BEWARE!

A typical phishing scam is a three step process:

1) The phisher deploys a web site which mimics portions of a legitimate financial institution or other e-commerce web site.

2) The phisher crafts an e-mail message which appears to be from the organization represented on the phishing web site. The e-mail message notifies the potential victim of a problem with their account and instructs them to login to the phishing site where the account information will be "verified".

3) Utilizing spam, the phisher sends this e-mail to hundreds of thousands of potential victims. If the victim falls for the scam, they end up divulging their account, credit card, and other identity theft related information. This information is then collected by the phisher and used to commit credit card fraud and other identity theft related offenses.

A new phishing technique adds another step to the process. It utilizes the login credentials entered by the victim to connect to the authentic web site and downloads unique identifying victim information such as first and last name. This data is then used to populate portions of the phishing web site. By doing so, the phishing site appears more legitimate; therefore, the victim is more likely to divulge sensitive information.

If you have received a fraud, or similar e-mail, please file a complaint at www.IC3.gov.